INDIANA UNIVERSITY

Charter
Information Security and Privacy Risk Council

Effective:	*May 4, 2011*
Last Updated:	*November 10, 2015*
Responsible University Office:	*University Information Security Office*
Responsible University Administrators:	*Vice President for Information Technology and Chief Information Officer* *Executive Vice President for University Academic Affairs*
Contacts:	***Information Security:*** *Tom Davis* *812-855-UISO* *uiso@iu.edu* ***Information Privacy:*** *Sara Chambers* *812-855-UIPO* *uipo@iu.edu*
Web Address:	https://protect.iu.edu/online-safety/program/governance.html
Related Information:	Indiana University Information Security and Privacy Program
History:	November 2015, corrected contacts, web addresses, and office names May 2011, new charter

Purpose

The Information Security and Privacy Risk Council ("the Council") operates under the auspices of the Office of the Vice President for Information Technology and CIO (for digital information protection and privacy) and the Office of the Executive Vice President for University Academic Affairs (for information and privacy in the physical world, and general policy and compliance). It is a standing committee providing broad strategic guidance and oversight to support the university-wide Indiana University Information Security and Privacy Program ("ISPP"). The ISPP exists to establish risk-based *safeguards* that adequately protect information, but do not unnecessarily impede its appropriate and widespread use.

Charter

The Information Security and Privacy Risk Council will:

- Develop, seek wide input, and recommend *strategic direction* to the Chief Security Officer and Chief Privacy Officer on university-wide information security and privacy.
- Review and coordinate university-wide information security and privacy-related policies, procedures, and initiatives, regardless of the office or *sector* responsible.
- Review and coordinate university-wide efforts to improve employee awareness of information security and privacy practices, regardless of the office or *sector* responsible.
- Provide strategic input to key information security and privacy projects undertaken by the University Information Security Office, the University Information Policy Office, and offices having compliance or monitoring responsibilities for the information security and privacy of particular *sectors*.
- Advise university administration on matters of information security and privacy, and with respect to compliance requirements.
- Stay abreast of emerging information security and privacy issues and adjust strategy as necessary.

The Council will strive to ensure that information security and privacy efforts support the university's mission, improve the overall security and privacy of information at IU, appropriately balance risk with *safeguards*, and are appropriately supported, funded and implemented within the university community.

Members are to fully own the process and results of the Council. Members will strive to ensure that the university-wide strategies promulgated by the Council and published in the ISPP support and complement *sector*-specific requirements and needs while still facilitating the widespread and appropriate use of information.

The Council shall have all authority necessary to fulfill the duties and responsibilities assigned to the Council in this Charter or otherwise assigned by the executive sponsors.

The Chief Privacy Officer and Chief Security Officer are responsible for reporting to university administration on the activities of the Council, and on general information security and privacy affairs.

Membership

The Council is chaired jointly by the Chief Security Officer and the Chief Privacy Officer, whose offices provide administrative support for the Council and apply the strategies identified by the Council to the ISPP. These two officers share ultimate responsibility for establishing and maintaining the Indiana University Information Security and Privacy Program.

The members of the Council are appointed by the Vice President for Information Technology and Chief Information Officer, and the Executive Vice President for University Academic Affairs, who jointly serve as the Council's executive sponsors.

Standing Members include those who, by virtue of their university role, have compliance or oversight responsibility for the information security and/or privacy policies, procedures, initiatives, and activities within their *sectors*, and in some cases in areas that cut across *sectors*. *Sectors* to be represented are those for which laws, regulations, standards, and/or contractual requirements make it prudent for Indiana University to address information security and/or privacy risks as a university-wide strategy. Standing Members are responsible for disseminating information about and ensuring the implementation of the work of the Council within the area over which they exercise security or privacy or other compliance oversight. Membership of the Council is reviewed periodically, but no less than every two years.

Others who have strategic expertise and background relevant to the information security and privacy needs of the university may be appointed as At-Large Members to two-year terms on the Council.

The Council may also invite independent experts or advisors to meetings as it deems necessary or appropriate, to advise the Council on specific matters and issues.

Procedures

Chairs and Members are appointed by letter by the Vice President for Information Technology and Chief Information Officer, and the Executive Vice President for University Academic Affairs.

Definitions

Safeguards are the administrative (e.g., policies, procedures, awareness, training), technical (e.g. passwords, access privileges), and physical (e.g. door locks, backup power) measures put in place to protect information.

A *sector* is a subset of the business of the university, whose components share similar characteristics. Examples of *sectors* include academic, financial, human resources, medical, research, and technology.

To provide *strategic direction* is to articulate and assess the principles, policies, and preferences that are to be promulgated at IU, with respect to information security and privacy.